



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,547	10/14/2003	J. Scott Carr	098888-1813	3480
99103 7590 04/06/2012 Foley & Lardner LLP 150 EAST GILMAN STREET P.O. BOX 1497 MADISON, WI 53701-1497			EXAMINER TRUVAN, LEYNN A THANH	
			ART UNIT 2435	PAPER NUMBER
			MAIL DATE 04/06/2012	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/686,547

Applicant(s)

CARR ET AL.

Examiner

LEYNNA TRUVAN

Art Unit

2435

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 November 2011.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1-12, 14-20, 25-29 and 58-63 is/are pending in the application.
- 5a) Of the above claim(s) 21-24 and 30-51 is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-12, 14-20 and 25-29, 58-63 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB08)
Paper No(s)/Mail Date ____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date ____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: ____

DETAILED ACTION

1. Claims 1-12, 14-20, 25, 27-29 and 58-64 are pending. Claims 58-64 are new.
Claims 13, 26 and 52-57 are cancelled by applicant.
Claims 21-24 and 30-51 are withdrawn by applicant.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/23/2011 has been entered.

Response to Arguments

3. Applicant's arguments filed 3/9/11 have been fully considered but they are not persuasive.

In response to argument on pg.18, applicant disagrees stating Wu shows (FIGS 4-6) merely disclose extracting biometrics from a working area of a document. FIG.4 specifically step 404 is "extract (biometric) feature and step 410 "extract watermark" step 412 is "verify watermark" which leads to step 414 "correlate" both the encrypted

extracted biometrics feature and watermark. Therefore, is not merely extracting biometrics but also verified the watermarking by correlating or in terms of comparing the extracted biometrics feature. Further, Wu teach verification can be done at different levels based on different requirements of particular applications (Wu-col.7, lines 15-219). Additionally, Maloney teach a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (Maloney-col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (Maloney-col.4, line 61-col.5, line 11 and col.5, lines 38-56). Therefore, it's obvious for a person of ordinary skills in the art that the Wu and Maloney combination teaches verification with the biometric capture method to authenticate and verify the age is appropriate or inappropriate and determines the document or an identification card is valid.

In response to argument on pg.19-21, that Wu and Maloney do not whatsoever disclose or suggest "verifying the bearer's age... biometric sample is physically captured from the bearer" and that Maloney fails to cure the deficiencies of Wu. Wu disclose the method and a device of verifying an age of a bearer of a document and inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious

biometric data is physically captured from the bearer/person. Additionally, Wu discloses verifying the biometric sample, watermark, and age of the bearer on the identification document (card) but does not specify the bearer is at least as old as a predetermined age. Thus, Maloney is brought forth to further disclose a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21 and col.5, lines 38-56). Therefore, Maloney does cure the deficiency of Wu to teach a device consist a multi-purpose processor receiving information from the identification document to perform the act of comparing and verifying the bearer's age when the first digital data indicates that the bearer is at least as old as a predetermined age because to perform the functions of verifying the age is appropriate or inappropriate and determines the identification card is valid (Maloney- col.1, lines 47-59 and col.2, lines 5-21).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-12,14-20, 25, 27-29 and 58-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wu, et al. (US 6,748,533) in view of Maloney, et al. (US 6,119,932).

As per claim 1:

Wu discloses a method of verifying an age of a bearer of a document, said method comprising:

receiving, at a processor, first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document; (col.7, line 65 – col.8, line 3)

receiving second digital data corresponding to a biometric indicator, the second digital data being obtained from auxiliary data steganographically embedded in the document; (col.3, lines 5-25 and col.6, lines 28-55)

receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer, and the biometric sample is physically captured from the bearer; and (col.10, lines 53-67 and col.11, lines 5-13)

verifying the bearer's age when: *i) the first digital data indicates that the bearer is at least as old as a predetermined age* (col.7, lines 20-28), and *ii) the second digital data and the third digital data correspond*. (col.5, lines 14-33 and col.9, lines 1-22)

Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where

this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss the first digital data indicates that the bearer is at least as old as a predetermined age.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured image, a microprocessor and a data detection device coupled to the microprocessor. (col.1, lines 47-59). Maloney also discusses a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5, line 11 and col.5, lines 38-56). Therefore it would have been obvious for a person of ordinary skills in the art to combine Wu with Maloney to teach the first digital data indicates that the bearer is at least as old as a predetermined age because this verifies the age is appropriate or inappropriate and determines the identification card is valid (Maloney-col.2, lines 5-21 and col.5, lines 38-56).

As per claim 2: See Wu on Fig.3 and Maloney on col.3, lines 25-60; discussing the method of claim 1, further comprising interrogating a data repository with the biometric indicator to obtain digital data being obtained from auxiliary data steganographically embedded in the document.

As per claim 3: See Wu on col.7, line 65 – col.8, line 3 and Maloney on col.5, lines 38-56; discussing the method of claim 2, further comprising interrogating the data repository with the age indicator to obtain the first digital information.

As per claim 4: See Wu on col.3, lines 5-15 and col.7, line 20-67 and Maloney on col.3, lines 25-60; discussing the method of claim 2, wherein the second digital data comprises a biometric template associated with the bearer.

As per claim 5: See Wu on col.7, line 20– col.8, line 3 and Maloney on col.3, lines 25-60; discussing the method of claim 4, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

As per claim 6: See Wu on col.7, line 55 – col.8, line 3; discussing the method of claim 1, wherein the third digital data is received through a network.

As per claim 7: See Wu on col.7, line 55 – col.8, line; discussing the method of claim 6, wherein the network comprises the internet.

As per claim 8: See Wu on col.7, line 55 – col.8, line 3; discussing the method of claim 1, wherein the biometric indicator comprises a biometric template.

As per claim 9: See Wu on Fig.3 and Maloney on col.3, lines 25-60; discussing the method of claim 8, wherein the biometric template includes information associated with

at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

As per claim 10: See Maloney on col.5, lines 6-11; discussing the method of claim 1, wherein the third digital data further comprises a timestamp.

As per claim 11: See Wu on col.7, lines 20-67 and col.11, lines 5-18; discussing the method of claim 4, wherein the auxiliary data comprises plural bits of data and wherein the biometric indicator and the age indicator comprise the same plural bits.

As per claim 12:

Wu discloses a method of anonymously verifying an age or characteristic associated with a person, associated with an identification document, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person, the method: (see Figs.1 and 6)

receiving optical scan data corresponding to the identification document, the optical scan data being generated by an optical sensor; (col.10, lines 53-67 and col.11, lines 5-13)

decoding the scan data with *a configured multi-purpose electronic processor* (col.2, lines 35-42) to obtain the first set of information included in the digital watermark, the first set of information including a concatenated string of data comprising age indicator and additional data, wherein the digital watermark is embedded in the identification document (col.4, lines 28-30 and col.5, lines 10-33) through hidden

changes to data representing one or more items carried by the identification document;
(col.3, lines 5-25 and col.6, lines 28-55)

receiving second optical scan data physically captured from the person
associated with the identification document;

verifying the identification document based on the second optical scan data and
the additional data; and

*determining, based on the first set of information, the person's age or age level in
connection with an age-related transaction or event* (col.7, lines 53-67 and col.8, lines 1-
48), wherein said act of determining protects the anonymity of the person in possession
of the identification document from said multi-purpose electronic processor or entity
performing said determining. (col.7, lines 20-28 and col.7, line 65 – col.8, line 3)

Wu discloses generating an invisible watermark and embedding the watermark
on an article or document (col.3, lines 5-25 and col.6, lines 28-31). The claimed
reduced-bit representation can broadly be interpreted as a watermarked representation
or encrypted/encoded data form. Wu teaches using encrypted information and seeds
(col.2, lines 5-22) for generating a watermark is obtained from a portion of an article or
document (col.7, lines 35-37 and col.8, lines 4-7). Wu further discloses the method of
generating a watermark involves this information is encrypted and a random pattern is
generated (col.4, lines 20-27 and col.11, lines 20-40). Thus, the watermark or
encrypted data is given as the claimed reduced-bit representation that was generated
from a portion of the document reads on the claimed generating a reduced-bit
representation of the received information carried by the document. The biometrics

data or information and other appending information alone or together can be provided as input that will identify invariant features. The invariant features have a size of a few hundred bites which is given as the claimed identification document comprising plural bits (col.11, lines 5-18). Wu discloses embedding various information that includes identification portion in various portions of the document (col.7, lines 20-28) such as an identification, name of the person, fingerprint, and personal particulars such as age and height (col.7, line 65 – col.8, line 3). Wu discusses inputting facial image in a facial recognition engine (col.10, lines 53-67) and the authentication or verification process is carried out until all portions of the article are checked (col.9, lines 1-22). Wu discloses a device for controlling repeated operations of extracting, encrypting, and for generating a watermark (col.2, lines 35-42). Wu obviously suggests that the device includes a processor in order to perform and carry out the functions of a device. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss a multi-purpose processor receiving information from the identification document and determining the person's age or age level in connection with an age-related transaction or event.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured image, a microprocessor and a data detection device coupled to the microprocessor.

The microprocessor has an associated memory structure, and the data detection device is operable to extract data from an identification card presented by the user and also includes a device for superimposing selected portions of the extracted data upon the captured image of the user (col.1, lines 47-59). The claimed identification document can be in the form of an identification card. The data detection device 24 (FIG. 1A) maybe a triple-track magnetic stripe reader that is coupled through a wedge decoder 30 to a video interface 32 that receives inputs from the camera 20. An output of the video interface 32 is connected to the storage device 22 and the wedge decoder 30 is also coupled to a microprocessor 26 having an associated memory structure 28 (col.2, line 66-col.3, line 9). Maloney discloses the customer present an identification card to the operator, who uses the data detection device 24 to read data from the identification card. The data is decoded by the decoder 30 and then transmitted to the microprocessor 26 and the video interface 32 (col.4, lines 33-38). Maloney further discusses a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5, line 11 and col.5, lines 38-56).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Maloney with Wu to teach a device consist a multi-purpose processor

receiving information from the identification document to perform the act of comparing because to perform the functions of verifying the age is appropriate or inappropriate and determines the identification card is valid (Maloney- col.1, lines 47-59 and col.2, lines 5-21).

As per claim 14: See Wu on col.7, line 53 – col.8, line 3; discussing the method of claim 12, wherein the identification document further comprises a second set of information embedded therein, the second set of information corresponding to a third set of information that is printed on the identification document, wherein the second set of information comprises an index for accessing a data repository.

As per claim 15: See Wu on col.8, lines 22-30; discussing the method of claim 14, wherein the index comprises a hash of the third set of information that is printed on the identification document.

As per claim 16: See Wu on col.1, lines 44-52 and col.8, lines 22-30; discussing the method of claim 14, further comprising computing a hash of the third set of information that is printed on the identification document, decoding the second set of information that is embedded in the identification document to obtain the embedded hash, and comparing the computed hash and the embedded hash to determine authenticity of the document.

As per claim 17: See Wu on col.7, lines 20-27 and Maloney on col.4, lines 34-46; discussing the method of claim 12, further comprising storing at least a portion of the first set of information in at least one of a list, electronic memory circuits and a data record, wherein the stored portion of the first set of information serves as an audit clue

to evidence that the identification document has been examined.

As per claim 18: See Wu on col.11, lines 15-18 and see FIG.6; discussing the method of claim 17, wherein the first set of information comprises two or more random bits.

As per claim 19: See Wu on col.7, lines 20-30; discussing the method of claim 18, wherein the first set of information comprises a date of birth.

As per claim 20: See Wu on col.11, lines 15-18 and see FIG.6; discussing the method of claim 19, wherein a combination of the random bits and the date of birth decrease likelihood of overlapping birth dates, while maintaining an anonymous audit clue.

As per claim 25:

Wu discloses a method comprising:

receiving optical scan data that is associated with an identification document (col.3, lines 29-42 and Fig.6), the identification document comprising plural-bits of data carried by the identification document (col.7, lines 35-37 and col.11, lines 5-18), wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document (col.3, lines 5-18 and col.6, lines 48-64) and the second field corresponding to an age or age level of the bearer of the identification document; (col.7, line 25 – col.8, line 3)

receiving information corresponding to the bearer based on the first field; (col.7, lines 15-19)

receiving second optical scan data physically captured from the bearer; (col.10, lines 55-62)

verifying the identification document based on the first field and the second optical scan data; (col.7, lines 20-29)

utilizing a configured multi-purpose electronic processor (col.2, lines 35-42), decoding the optical scan data to recover corresponding to at least the second field; (col.1, lines 45-53)

receiving information carried by the document (col.2, lines 5-22 and col.8, lines 4-7), separate from the data corresponding to at least the second field and generating a reduced-bit representation of the received information by *using a configured multi-purpose electronic processor;* and (col.4, lines 20-27 and col.11, lines 20-40)

comparing data corresponding to the second field with the reduced-bit representation (col.5, lines 1-34 and col.9, lines 1-22) to verify an age level associated with the document in connection with an age-related transaction or event, (col.7, lines 53-67 and col.8, lines 1-48)

wherein neither the data corresponding to the second field nor the reduced-bit representation, betray the identity of the bearer of the identification document to said *multi-purpose electronic processor or an entity performing said act of comparing.* (col.12, lines 1-9 and 44-67 and col.13, lines 15-27)

Wu further discloses the method of generating a watermark involves this information is encrypted and a random pattern is generated (col.4, lines 20-27 and col.11, lines 20-40). Thus, the watermark or encrypted data is given as the claimed

reduced-bit representation that was generated from a portion of the document reads on the claimed generating a reduced-bit representation of the received information carried by the document. The biometrics data or information and other appending information alone or together can be provided as input that will identify invariant features. The invariant features have a size of a few hundred bites which is given as the claimed identification document comprising plural bits (col.11, lines 5-18). Wu discloses embedding various information that includes identification portion in various portions of the document (col.7, lines 20-28) such as an identification, name of the person, fingerprint, and personal particulars such as age and height (col.7, line 65 – col.8, line 3). Wu discusses inputting facial image in a facial recognition engine (col.10, lines 53-67) and the authentication or verification process is carried out until all portions of the article are checked (col.9, lines 1-22). Wu discloses a device for controlling repeated operations of extracting, encrypting, and for generating a watermark (col.2, lines 35-42). Wu obviously suggests that the device includes a processor in order to perform and carry out the functions of a device. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss a multi-purpose processor receiving information from the identification document to perform the act of comparing.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured

image, a microprocessor and a data detection device coupled to the microprocessor. The microprocessor has an associated memory structure, and the data detection device is operable to extract data from an identification card presented by the user and also includes a device for superimposing selected portions of the extracted data upon the captured image of the user (col.1, lines 47-59). The claimed identification document can be in the form of an identification card. The data detection device 24 (FIG. 1A) maybe a triple-track magnetic stripe reader that is coupled through a wedge decoder 30 to a video interface 32 that receives inputs from the camera 20. An output of the video interface 32 is connected to the storage device 22 and the wedge decoder 30 is also coupled to a microprocessor 26 having an associated memory structure 28 (col.2, line 66-col.3, line 9). Maloney discloses the customer present an identification card to the operator, who uses the data detection device 24 to read data from the identification card. The data is decoded by the decoder 30 and then transmitted to the microprocessor 26 and the video interface 32 (col.4, lines 33-38). Maloney further discusses a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5, line 11 and col.5, lines 38-56).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Maloney with Wu to teach a device consist a multi-purpose processor receiving information from the identification document to perform the act of comparing because this executes the functions of verifying the identification card is valid (Maloney-col.1, lines 47-59 and col.2, lines 5-21).

As per claim 27: See Wu on col.7, lines 35-37 and col.4, lines 48-55; discussing the method of claim 25, further comprising storing the data corresponding to the second field in a data repository to evidence examination of the identification document.

As per claim 28: See Wu on col.8, lines 63-67; discussing the method of claim 25, further comprising printing the data corresponding to the second field to evidence examination of the identification document.

As per claim 29: See Wu on col.1, lines 45-50 and Maloney on col.3, lines 25-30; discussing the method of claim 25, wherein said receiving information carried by the document comprises receiving data corresponding to at least one of data generated by a barcode scanner, optical character recognizer, manual entry or watermark decoder.

As per claim 57:

Wu discloses an apparatus comprising:

a processor configured to:

receive first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document;
(col.7, line 65 – col.8, line 3)

receive second digital data corresponding to a biometric indicator, the second digital data being obtained from auxiliary data steganographically embedded in the document; (col.3, lines 5-25 and col.6, lines 28-55)

receive third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer, and the biometric sample is physically captured from the bearer; and (col.10, lines 53-67 and col.11, lines 5-13)

verify the bearer's age (col.7, lines 20-28) when: *i) the first digital data indicates that the bearer is at least as old as a predetermined age*, and *ii) the second digital data and the third digital data correspond*. (col.5, lines 14-33 and col.9, lines 1-22)

Wu discloses generating an invisible watermark and embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other unauthorized modification (col.12, lines 48-53). Wu discloses one or several invariant features combined can encrypted by hashing or to produce a random pattern using the extracted message and combine the original content and the generated pattern to generate a watermark (col.8, lines 28-30 and col.9, lines 43-45). Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such

as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss verifying the bearer's age when: i) the first digital data indicate that the bearer is at least as old as a predetermined age.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured image, a microprocessor and a data detection device coupled to the microprocessor. (col.1, lines 47-59). Maloney also discusses a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5, line 11 and col.5, lines 38-56). Therefore it would have been obvious for a person of ordinary skills in the art to combine Wu with Maloney to teach verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age because this verifies the age is appropriate or inappropriate and determines the identification card is valid (Maloney-col.2, lines 5-21 and col.5, lines 38-56).

As per claim 59:

Wu discloses a non-transitory computer-readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations comprising:

receiving first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document; (col.7, line 65 – col.8, line 3)

receiving second digital data corresponding to a biometric indicator, the second digital data being obtained from auxiliary data steganographically embedded in the document; (col.3, lines 5-25 and col.6, lines 28-55)

receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer, and the biometric sample is physically captured from the bearer; and (col.10, lines 53-67 and col.11, lines 5-13)

verifying the bearer's age (col.7, lines 20-28) when: i) *the first digital data indicates that the bearer is at least as old as a predetermined age*, and ii) the second digital data and the third digital data correspond. (col.5, lines 14-33 and col.9, lines 1-22)

Wu discloses generating an invisible watermark and embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other unauthorized modification (col.12, lines 48-53). Wu discloses one or several invariant features combined can encrypted by hashing or to produce a random pattern using the extracted message and combine the original content and the generated pattern to generate a watermark (col.8, lines 28-30 and col.9,

lines 43-45). Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss verifying the bearer's age when: i) the first digital data indicate that the bearer is at least as old as a predetermined age.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured image, a microprocessor and a data detection device coupled to the microprocessor. (col.1, lines 47-59). Maloney also discusses a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5,

line 11 and col.5, lines 38-56). Therefore it would have been obvious for a person of ordinary skills in the art to combine Wu with Maloney to teach verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age because this verifies the age is appropriate or inappropriate and determines the identification card is valid (Maloney-col.2, lines 5-21 and col.5, lines 38-56).

As per claim 60:

Wu discloses an apparatus comprising: a processor configured to:

receive optical scan data corresponding to an identification document, the optical scan data being generated by an optical sensor, wherein the identification document is associated with a person, the identification document including a document layer and printing carried by the document layer (col.7, line 65 – col.8, line 3), the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person; (col.3, lines 5-25 and col.6, lines 28-55)

decode the scan data to obtain the first set of information included in the digital watermark (col.5, lines 11-12), the first set of information including a concatenated string of data comprising an age indicator and additional data (col.10, lines 53-67 and col.11, lines 5-13), wherein the digital watermark is embedded in the identification document through hidden changes to data representing one or more items carried by the identification document; (col.8, lines 28-30 and col.9, lines 43-45)

receiving second optical scan data physically captured from the person associated with the identification document; (col.7, lines 15-19 and col.10, lines 55-62)
verifying the identification document based on the second optical scan data and the additional data; and(col.7, lines 20-29)

determine, based on the first set of information (col.7, lines 20-28), the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from the processor or and entity associated with said determining. (col.5, lines 14-33 and col.9, lines 1-22)

Wu discloses generating an invisible watermark and embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other unauthorized modification (col.12, lines 48-53). Wu discloses one or several invariant features combined can encrypted by hashing or to produce a random pattern using the extracted message and combine the original content and the generated pattern to generate a watermark (col.8, lines 28-30 and col.9, lines 43-45). Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such

as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss determining, based on the first set of information the person's age or age level in connection with an age-related transaction or event.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured image, a microprocessor and a data detection device coupled to the microprocessor. (col.1, lines 47-59). Maloney also discusses a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5, line 11 and col.5, lines 38-56). Therefore it would have been obvious for a person of ordinary skills in the art to combine Wu with Maloney to teach determining, based on the first set of information the person's age or age level in connection with an age-related transaction or event because this verifies the age is appropriate or inappropriate and determines the identification card is valid (Maloney-col.2, lines 5-21 and col.5, lines 38-56).

As per claim 61:

Wu discloses a non-transitory computer-readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations comprising:

receiving optical scan data corresponding to an identification document, the optical scan data being generated by an optical sensor, wherein the identification document is associated with a person, the identification document including a document layer and printing carried by the document layer (col.7, line 65 – col.8, line 3), the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information (col.8, lines 28-30 and col.9, lines 43-45), the first set of information including information to verify age or an age level of the person; (col.3, lines 5-25 and col.6, lines 28-55)

decoding the scan data to obtain the first set of information included in the digital watermark (col.5, lines 10-11), the first set of information including a concatenated string of data comprising an age indicator and additional data (col.10, lines 53-67 and col.11, lines 5-13), wherein the digital watermark is embedded in the identification document through hidden changes to data representing one or more items carried by the identification document; and (col.8, lines 28-30 and col.9, lines 43-45)

receiving second optical scan data physically captured from the person associated with the identification document; (col.7, lines 15-19 and col.10, lines 55-62)

verifying the identification document based on the second optical scan data and the additional data; (col.7, lines 20-29)

determining, based on the first set of information (col.7, lines 20-28), *the person's age or age level in connection with an age-related transaction or event*, wherein said act of determining protects the anonymity of the person in possession of the identification document from the computing device or and entity associated with said determining. (col.5, lines 14-33 and col.9, lines 4-21)

Wu discloses generating an invisible watermark and embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other unauthorized modification (col.12, lines 48-53). Wu discloses one or several invariant features combined can encrypted by hashing or to produce a random pattern using the extracted message and combine the original content and the generated pattern to generate a watermark (col.8, lines 28-30 and col.9, lines 43-45). Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss determining,

based on the first set of information the person's age or age level in connection with an age-related transaction or event.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured image, a microprocessor and a data detection device coupled to the microprocessor. (col.1, lines 47-59). Maloney also discusses a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5, line 11 and col.5, lines 38-56). Therefore it would have been obvious for a person of ordinary skills in the art to combine Wu with Maloney to teach determining, based on the first set of information the person's age or age level in connection with an age-related transaction or event because this verifies the age is appropriate or inappropriate and determines the identification card is valid (Maloney-col.2, lines 5-21 and col.5, lines 38-56).

As per claim 62:

Wu discloses an apparatus comprising: a processor configured to:
receive optical scan data that is associated with an identification document, the identification document comprising plural-bits of data carried by the identification

document (col.7, line 65 – col.8, line 3), wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document and the second field corresponding to an age or age level of the bearer of the identification document; (col.3, lines 5-25 and col.6, lines 28-55)

receiving information corresponding to the bearer based on the first field; (col.7, lines 15-19)

receiving second optical scan data physically captured from the bearer; (col.10, lines 55-62)

verifying the identification document based on the first field and the second optical scan data; (col.7, lines 20-27)

decode the optical scan data to recover data corresponding to at least the second field; (col.4, lines 29-30)

receive information carried by the document, separate from the data corresponding to at least the second field, and generating a reduced-bit representation of the received information; and (col.8, lines 28-30 and col.9, lines 43-45)

compare data corresponding to the second field with the reduced-bit representation (col.7, lines 20-28) *to verify an age level associated with of the document in connection with an age-related transaction or event*, wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to the processor or an entity performing said act of comparing. (col.5, lines 14-33 and col.6, lines 32-35)

Wu discloses generating an invisible watermark and embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other unauthorized modification (col.12, lines 48-53). Wu discloses one or several invariant features combined can encrypted by hashing or to produce a random pattern using the extracted message and combine the original content and the generated pattern to generate a watermark (col.8, lines 28-30 and col.9, lines 43-45). Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss to verify an age level associated with of the document in connection with an age-related transaction or event.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured image, a microprocessor and a data detection device coupled to the microprocessor. (col.1, lines 47-59). Maloney also discusses a method of vending a product having a

minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5, line 11 and col.5, lines 38-56). Therefore it would have been obvious for a person of ordinary skills in the art to combine Wu with Maloney to teach to verify an age level associated with of the document in connection with an age-related transaction or event because this verifies the age is appropriate or inappropriate and determines the identification card is valid (Maloney-col.2, lines 5-21 and col.5, lines 38-56).

As per claim 63:

Wu discloses a non-transitory computer-readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations comprising:

receiving first optical scan data that is associated with an identification document, the identification document comprising plural-bits of data carried by the identification document (col.7, line 65 – col.8, line 3), wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document and the second field corresponding to an age or age level of the bearer of the identification document; (col.3, lines 5-25 and col.6, lines 28-55)

receiving information corresponding to the bearer based on the first field; (col.7, lines 15-19)

receiving second optical scan data physically captured from the bearer; (col.10, lines 55-62)

verifying the identification document based on the first field and the second optical scan data; (col.7, lines 20-28)

decoding the optical scan data to recover data corresponding to at least the second field; (col.4, lines 29-30)

receiving information carried by the document, separate from the data corresponding to at least the second field, and generating a reduced-bit representation of the received information; and (col.8, lines 28-30 and col.9, lines 43-45)

comparing data corresponding to the second field with the reduced-bit representation (col.7, lines 20-28) *to verify an age level associated with of the document in connection with an age-related transaction or event*, wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to the computing device or an entity performing said act of comparing. (col.5, lines 14-33 and col.6, lines 32-35)

Wu discloses generating an invisible watermark and embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other unauthorized modification (col.12, lines 48-53). Wu discloses one or several invariant features combined can encrypted by hashing or to produce a random pattern using the extracted message and combine the original

content and the generated pattern to generate a watermark (col.8, lines 28-30 and col.9, lines 43-45). Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Wu discloses inputs of biometric data such as a person's facial image or fingerprint (col.10, lines 55-62). Biometric data such as facial or fingerprints are known to be taken or captured via a device directly from and of a person's face, fingers, hand, etc. Thus, is obvious biometric data is physically captured from the bearer/person. However, Wu did not clearly discuss to verify an age level associated with of the document in connection with an age-related transaction or event.

Maloney discloses an improved identification verification apparatus comprises a camera for capturing an image of a user, a storage device that stores the captured image, a microprocessor and a data detection device coupled to the microprocessor. (col.1, lines 47-59). Maloney also discusses a method of vending a product having a minimum age limitations where data is extracted from an identification card. The extracted information includes data of birth information that is used to calculate whether the identification card indicates that the user satisfies the minimum age limitation. Thus determines the identification card is valid (col.2, lines 5-21). The age calculation is performed by the verification apparatus to determine whether or not the

person/customer has the appropriate or of not an appropriate age (col.4, line 61-col.5, line 11 and col.5, lines 38-56). Therefore it would have been obvious for a person of ordinary skills in the art to combine Wu with Maloney to teach to verify an age level associated with of the document in connection with an age-related transaction or event because this verifies the age is appropriate or inappropriate and determines the identification card is valid (Maloney-col.2, lines 5-21 and col.5, lines 38-56).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA TRUVAN whose telephone number is (571)272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 6:00PM) and telework on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T./
Examiner, Art Unit 2435

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435